UNIVERSITÀ DEGLI STUDI
DI TRENTO

DEPARTMENT OF INFORMATION ENGINEERING AND COMPUTER SCIENCE

ICT International Doctoral School

Scalable Safety and Reliability Analysis via Symbolic Model Checking: Theory and Applications

Cristian Mattarei

Advisor

Alessandro Cimatti

Head of Embedded Systems Unit,

Fondazione Bruno Kessler

Co-Advisor

Marco Bozzano

Senior Researcher,

Fondazione Bruno Kessler

February 2016

UNIVERSITÀ DEGLI STUDI
DI TRENTO

DEPARTMENT OF INFORMATION ENGINEERING AND COMPUTER SCIENCE

ICT International Doctoral School

PhD Committee

David Jones
The Boeing Company

Luigi Portinale
University of Piemonte Orientale

Roberto Sebastiani
University of Trento

Christel Seguin
ONERA

Joseph Sifakis
EPFL

Abstract

Assuring safety and reliability is fundamental when developing a safety critical system. Road, naval and avionic transportation; water and gas distribution; nuclear, eolic, and photovoltaic energy production are only some examples where it is mandatory to guarantee those properties. The continuous increasing in the design complexity of safety critical system calls for a never ending sought of new and more advanced analytical techniques. In fact, they are required to assure that undesired consequences are highly improbable.

In this Thesis we introduce a novel methodology able to raise the bar in the area of automated safety and reliability analysis. The proposed approach integrates a series of techniques, based on symbolic model checking, into the current development process of safety critical systems. Moreover, our methodology and the resulting techniques are thereafter applied to a series of real-world case studies, developed in collaboration with authoritative entities such as NASA and the Boeing Company.

Keywords

[Model-Based Safety Assessment, Symbolic Model Checking, Safety Assessment, Reliability Analysis, Fault Tree Analysis, Contract-Based Design, Minimal Cutsets]

Contents

List of Tables

List of Figures

List of Acronyms

ATC	Air Traffic Control
BDD	Binary Decision Diagram
CBD	Contract-Based Design
CBSA	Contract-Based Safety Assessment
CD&R	Conflict Detection and Resolution
CS	Cutset
CTL	Computational Tree Logic
DAG	Directed Acyclic Graph
DMR	Double Modular Redundancy
FBW	Fly-by-Wire
FDIR	Fault Detection Identification and Recovery
FMEA	Fault Mode and Effects Analysis
FTA	Fault Tree Analysis
GSEP	Ground Separated Aircraft
IC3	Incremental Construction of Inductive Clauses for Indubitable Correctness
LTL	Linear Temporal Logic
MBSA	Model-Based Safety Assessment
MEA	More Electric Airplane

MCS Minimal Cutsets

PDR Property Directed Reachability

SMT Satisfiability Modulo Theory

SSEP Self Separated Aircraft

TMR Triple Modular Redundancy

V&V Validation and Verification

WBS Wheel Braking System

1

Introduction

If a machine is expected to be infallible,
it cannot also be intelligent.

– Alan Turing

It is the 1906, and Lee de Forest invents the vacuum tube and makes way for the active electronics. 30 years later, this result had a huge impact in WWII which pushed on this technology and initiated the electronic revolution. Colossus, the world's first programmable computer, was one of the most important application of such technology, but in this Thesis we refer to this period for a different reason: the emerging of safety and reliability engineering.

Electronic researches during WWII contributed in the development of technological applications such as radio, radar, and television. At the same time, the vacuum tubes were also the main cause of equipment failure, in fact they required to be replaced five times more often then all other equipments. This recurring issue required to investigate on the definition of specific analysis, able to attribute the cause of such unreliability of the electrical components. In a general perspective, the term reliability attributes to the system capability of behaving in accordance with its prescribed functionality, in fact a failure of a vacuum tube in an electrical

device can cause the entire system not to working property. Differently, system safety is the property of not causing damage, risk, or injury. After WWII, specific studies in this direction arose from the necessity to deal with the increasing level of complexity in military aircraft and ballistic missile systems.

Over the years, the vacuum tubes were replaced by transistors, and their successive miniaturization has allowed for the increasing in system capability and complexity. In parallel to this trend, safety and reliability engineering have had to evolve by introducing new and more efficient approaches able to support the design, and avoid unintended behaviors, of such complex systems. In the current era, the problem of assuring safety and reliability affects the design of systems that are definitely more pervasive than the purely military ones. Most notably areas of application for such disciplines are road, naval and avionic transportation; water and gas distribution; and nuclear, eolic, and photovoltaic energy production. Guaranteeing safety and reliability in these applications is mandatory, thus they are categorized as *safety critical systems*. The process that guides the development of a safety critical system is highly controlled and standardized by the competent authorities. In fact, releasing a certificate of system conformance requires to guarantee that system requirements, defined at the early stages of the development, are fairly derived into the system and sub-systems design, correctly implemented into the production phase, and - finally - that the concrete system implementation is in accordance with sub-systems, system, and the original requirements definition. Each of these phases is characterized by a set of well established analysis and methodology, which guides the system design through an incremental refinement from initial requirements definition to the final system implementation. The resulting process has two parallel flows: one that analyzes the system under normal conditions, and the other that evaluates its robustness in

presence of components' failure. The former is the system development *V-Model*, and the latter is called *safety assessment*.

Modern safety critical systems have become so complex that their safety cannot be shown solely by test, and whose logic is nearly impossible to comprehend without the aid of analytical tools. The approach that, in the last decades, emerged to cope with such complexity is the use of formal methods. In practice, a system behavior can be defined with a variety of diagrams, textual descriptions, and operational procedures, but in all cases they must be well defined and tailored to avoid ambiguous interpretations. The application of formal methods solves this issue by providing a set of mathematical based techniques that allow the engineer to discharge the possibility of introducing design misinterpretations. Since the resulting formal representation of the system has a unique interpretation, therefore it can be interpreted by a software that allows for automated or semi-automated analysis to discover design flaws, and to validate the result. The introduction of *model checking*, in early 1980s, represented one of the most important achievements in the field of formal methods. In fact, this technique allows for exhaustively and automatically check whether a formal system definition - the model - meets a set of formal requirements. However, while highly promising, model checking required several years to be effectively applied to a real-world scenario and be integrated into a development process.

In the 1990s, the advances of the model-based techniques have received significant interest in the community of safety and reliability engineering. The ensemble of those disciplines is defined as *model-based safety assessment* (MBSA). The objective of this research field is to support the analysis prescribed by the safety assessment process, by relying on the definition of a formal model of the system. In particular, original MBSA techniques [68, 100, 13] were directed to provide a single formalism able to automa-

tize the production of classical safety artifacts such as Fault Trees (FT) and Fault Modes and Effects Analysis (FMEA) tables. However, those approaches were operating only at the safety assessment level, and the relation with the nominal system analysis (i.e., the V-Model) was not considered.

The successive integration with model checking techniques allowed to reduce this gap [29, 39, 38, 42, 11, 22, 21, 37]. However, the resulting techniques were not directed to natively support the distinctive refinement of the design that characterizes the development of a safety critical system. At the same time, they experience significant issues when dealing with real-world, large scale system designs.

Contributions

In this Thesis we define a set of comprehensive model-based safety assessment methodologies and techniques able to overcome the limitations of current approaches. The proposed solution provides i) a seamless integration with standard V-Model and safety assessment processes, ii) able to natively follow the characteristic refinement of the system design, iii) by providing advanced and completely automated techniques for assuring system safety and reliability, iv) while guaranteeing the ability to deal with real-world system designs.

This target has been reached by integrating several different techniques into a single framework. The contributions of this Thesis that support these results are the followings:

- In [30] we improve the performance of the minimal cutsets computation, which represents the basis of all model-based safety assessment techniques that rely on symbolic model checking. This result has been possible via the application of modern SAT-based algorithms. Moreover, we widen the level of expressivity supported by the minimal

cutsets computation, moving from pure invariant definition of system specifications to a full support of Linear Temporal Logic (LTL) [102].

- In [35] we encompass an emerging paradigm called contract-based design (CBD) in order to define a novel methodology that natively supports the refinement of system design. In fact, CBD introduces a formal approach to automatically analyze the correctness of system decompositions into a hierarchy of sub-systems and modules.

- We extend current model-based safety assessment methodologies in order to support the reliability analysis of redundant architectures [33]. This approach integrates Satisfiability Modulo Theory (SMT) and minimal cutsets computation in order to support the analysis in the early stages of the system design e.g., when modules implementation have not yet defined. Moreover, in [34] we apply a specialized technique based on model abstraction that significantly improves the performance.

- We implemented all aforementioned techniques into a set of specialized tools such as nuXmv [97], xSAP [27], and OCRA [54], which are engineered in order to support a comprehensive framework that follows the system design by supporting both V-model and safety assessment processes.

- In order to validate the practical applicability of the methodologies introduced in this Thesis, we applied them to a series of real-world case studies. Most notably, the aforementioned approaches are applied in a joint project with the National Aeronautics and Space Agency (NASA) to formally analyze a series of possible designs for the next generation of the Air Traffic Control system (ATC) [90, 69]. Furthermore, an analysis of the reliability has been applied to the archi-

tectural design of the Primary Flight Computers of the Boeing 777 and Airbus A330. Moreover, we discuss the effectiveness of the proposed approach to produce safety analysis artifacts, by applying it to a case-study described in the Aerospace Information Report [109];

- We provide the whole documentation regarding case studies and tools at the link `www.mattarei.eu/cristian/thesis`.

Structure of the Thesis

The rest of this Thesis is organized as follows:

- Part I provides the background notions that identify the starting point of this Thesis. This Part provides an overview of V-Model and safety assessment processes, their integration with formal methods, and a set of formal definitions characterizing the problem that we intend to solve.
- Part II elaborates on the problem of minimal cutsets computation. The first portion describes how to relate nominal design and its extension with failure behaviors. Previous techniques are then discussed, in addition to a set of simple extensions that can be applied to solve this problem. This Part continues with the introduction of novel techniques that define the new state of the art in the minimal cutsets computation. An extensive experimental evaluation is then described, followed by the description of an LTL extension, and future directions.
- Part III describes the integration of safety analysis with contract-based design. In this Part we follow the description of the technique with a running example taken from an avionic standard. Subsequently, we provide a detailed definition of contract-based design, which is then extended into the contract-based safety analysis approach. This Part

concludes with an experimental evaluation and a discussion on future directions.

- Part IV elaborates on the techniques for the reliability analysis of redundant architectures. Firstly, it provides an overview of the techniques used to increase hardware reliability by the application of components redundancy. Afterwards, we provide the detail of the automated technique based on Satisfiability Modulo Theory, and its subsequent improvement based on predicate abstraction. Experimental evaluations and future directions conclude this Part.

- Part V is devoted at describing the tools architecture that we designed in order to carry out the aforementioned techniques. This Part describes the evolution that have been applied on nuXmv, xSAP, and OCRA tools in order to defined the model-based safety assessment approach described in this Thesis. A discussion on the resulting comprehensive process is then provided.

- Part VI supports the effectiveness of the techniques that we have introduced in this work, by providing the details of their application to a set of real-world case studies. In this Part we first describe the analysis of a triple modular generator, which is a small but representative example to introduce the application of model-based safety assessment. Afterwards, we provide the details of the evaluation of the next generation of the air traffic control system, the analysis of the Fly-by-Wire architectures of two modern aircraft, and an extract of the results reached on the evaluation of an avionic based wheel braking system.

Bibliography

[1] Martín Abadi and Leslie Lamport. Composing Specifications. *ACM Trans. Program. Lang. Syst.*, 15(1):73–132, 1993.

[2] Sherif Abdelwahed, Gabor Karsai, Nagabhushan Mahadevan, , and Stanley Ofsthun. Practical Implementation of Diagnosis Systems Using Timed Failure Propagation Graph Models. *IEEE T. Instrumentation and Measurement*, 58(2):240–247, 2009.

[3] Parosh Aziz Abdulla, Johann Deneux, Gunnar Stålmarck, Herman Ågren, and Ove Åkerlund. Designing Safe, Reliable Systems Using Scade. In *Leveraging Applications of Formal Methods, First International Symposium, ISoLA 2004, Paphos, Cyprus, October 30 - November 2, 2004, Revised Selected Papers*, pages 115–129, 2004.

[4] Ignasi Abío, Robert Nieuwenhuis, Albert Oliveras, and Enric Rodríguez-Carbonell. A Parametric Approach for Smaller and Better Encodings of Cardinality Constraints. In *Proceedings of CP*, 2013.

[5] Jacob A. Abraham and Daniel P. Siewiorek. An algorithm for the accurate reliability evaluation of triple modular redundancy networks. *IEEE Trans. on Comp.*, 100(7):682–692, 1974.

[6] Jean-Raymond Abrial. *The B-book: Assigning Programs to Meanings*. Cambridge Univ. Press, 1996.

[7] Federal Aviation Administration. Advisory Circular 20-174. http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%2020-174.pdf.

[8] Federal Aviation Administration. Advisory Circular 23-1309-1E. http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%2023.1309-1E.pdf.

[9] Federal Aviation Administration. System Design and Analysis Document Information, 2002. FAA Advisory Circular 25.1309-1.

[10] Airbus. A330, Flight Deck and Systems Briefing for Pilots, 1999. STL 472.755/92.

[11] Ove Åkerlund, Pierre Bieber, Eckard Boede, Marco Bozzano, Matthias Bretschneider, Charles Castel, Antonella Cavallo, Massimo Cifaldi, Jean Gauthier, Alain Griffault, et al. ISAAC, a framework for integrated safety analysis of functional, geometrical and human aspects. *Proc. ERTS*, 2006, 2006.

[12] Tom Anderson and Peter A Lee. *Fault tolerance, principles and practice*. Prentice/Hall International, 1981.

[13] André Arnold, Gérald Point, Alain Griffault, and Antoine Rauzy. The AltaRica formalism for describing concurrent systems. *Fundamenta Informaticae*, 40:109–124, 2000.

[14] Gilles Audemard, Piergiorgio Bertoli, Alessandro Cimatti, Artur Korniłowicz, and Roberto Sebastiani. A SAT based approach for solving formulas over boolean and linear mathematical propositions. In *Automated Deduction CADE-18*, pages 195–210. Springer, 2002.

[15] Richard Banach and Marco Bozzano. The Mechanical Generation of Fault Trees for Reactive Systems via Retrenchment II: Clocked and Feedback Circuits. *FAC*, 25(4):609–657, 2013.

[16] Iain Bate, Richard Hawkins, and John A. McDermid. A Contract-based Approach to Designing Safe Systems. In *SCS*, pages 25–36, 2003.

[17] Christophe Bauer, Kristen Lagadec, Christian Bès, and Marcel Mongeau. Flight control system architecture optimization for fly-by-wire airliners. *Journal of guidance, control, and dynamics*, 30(4):1023–1029, 2007.

[18] Saddek Bensalem, Vijay Ganesh, Yassine Lakhnech, César Munoz, Sam Owre, Harald Rueß, John Rushby, Vlad Rusu, Hassen Saıdi, Natarajan Shankar, et al. An overview of sal. In *Proceedings of the 5th NASA Langley Formal Methods Workshop*, 2000.

[19] Albert Benveniste, Benoit Caillaud, Alberto Ferrari, Leonardo Mangeruca, Roberto Passerone, and Christos Sofronis. Multiple Viewpoint Contract-Based Specification and Design. In *FMCO*, pages 200–225, 2007.

[20] Cinzia Bernardeschi, Alessandro Fantechi, Stefania Gnesi, Giorgio Mongardi, and Giorgio. Proving safety properties for embedded control systems, 1996.

[21] Pierre Bieber, Christian Bougnol, Charles Castel, Jean-Pierre Christophe Kehren, Sylvain Metge, and Christel Seguin. Safety assessment with altarica. In *Building the Information Society*, volume 156 of *IFIP International Federation for Information Processing*, pages 505–510. 2004.

[22] Pierre Bieber, Charles Castel, and Christel Seguin. Combination of Fault Tree Analysis and Model Checking for Safety Assessment of Complex System. In *Proc. EDCC-4*, volume 2485 of *LNCS*, pages 19–31. Springer, 2002.

[23] Armin Biere, Cyrille Artho, and Viktor Schuppan. Liveness checking as safety checking. *Electronic Notes in Theoretical Computer Science*, 66(2):160–177, 2002.

[24] Armin Biere, Alessandro Cimatti, Edmund M. Clarke, and Yunshan Zhu. Symbolic model checking without bdds. In *Proc. TACAS*, volume 1579 of *LNCS*, pages 193–207. Springer, 1999.

[25] Armin Biere and Keijo Heljanko. Hardware Model Checking Competition, 2015. http://fmv.jku.at/hwmcc15/.

[26] Armin Biere, Keijo Heljanko, and Siert Wieringa. *AIGER*, 2011. `http://fmv.jku.at/aiger/`.

[27] Benjamin Bittner, Marco Bozzano, Roberto Cavada, Alessandro Cimatti, Marco Gario, Alberto Griggio, Cristian Mattarei, Andrea Micheli, and Gianni Zampedri. The xsap safety analysis platform. In *Tools and Algorithms for Construction and Analysis of Systems (TACAS)*, Lecture Notes in Computer Science. Springer Verlag, 2015.

[28] Andrea Bondavalli, Mario Dal Cin, Diego Latella, István Majzik, András Pataricza, and Giancarlo Savoia. Dependability analysis in the early phases of UML-based system design. *Comput. Syst. Sci. Eng.*, 16(5):265–275, 2001.

[29] Marco Bozzano, Antonella Cavallo, Massimo Cifaldi, Laura Valacca, and Adolfo Villafiorita. Improving safety assessment of complex sys-

tems: An industrial case study. In *Proceedings of Formal Methods 2003 (LNCS 2805*, pages 208–222. Springer-Verlag, 2003.

[30] Marco Bozzano, Alessandro Cimatti, Alberto Griggio, and Cristian Mattarei. Efficient anytime techniques for model-based safety analysis. In *Computer Aided Verification - 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, Part I*, pages 603–621, 2015.

[31] Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, and Marco Roveri. Safety, dependability, and performance analysis of extended AADL models. *The Computer Journal*, doi: 10.1093/com, March 2010.

[32] Marco Bozzano, Alessandro Cimatti, Oleg Lisagor, Cristian Mattarei, Sergio Mover, Marco Roveri, and Stefano Tonetta. Safety Assessment of AltaRica Models via Symbolic Model Checking. *Science of Computer Programming*, 98(4):464 – 483, 2015.

[33] Marco Bozzano, Alessandro Cimatti, and Cristian Mattarei. Automated analysis of reliability architectures. In *ICECCS*, pages 198–207. IEEE Computer Society, 2013.

[34] Marco Bozzano, Alessandro Cimatti, and Cristian Mattarei. Efficient Analysis of Reliability Architectures via Predicate Abstraction. In *Proc. HVC*, number 8244 in LNCS, pages 279–294. Springer, 2013.

[35] Marco Bozzano, Alessandro Cimatti, Cristian Mattarei, and Stefano Tonetta. Formal Safety Assessment via Contract-Based Design. In *Proc. ATVA*, number 8837 in LNCS, pages 81–97. Springer, 2014.

[36] Marco Bozzano, Alessandro Cimatti, Anthony Fernandes Pires, David Jones, Greg Kimberly, Tyler Petri, Richard Robinson, and

Stefano Tonetta. A formal account of the AIR6110 Wheel Brake System. 2015. Submitted to CAV'15.

[37] Marco Bozzano, Alessandro Cimatti, and Francesco Tapparo. Symbolic fault tree analysis for reactive systems. In *ATVA*, pages 162–176, 2007.

[38] Marco Bozzano and Adolfo Villafiorita. Improving system reliability via model checking: The fsap/nusmv-sa safety analysis platform. In *SAFECOMP*, pages 49–62, 2003.

[39] Marco Bozzano and Adolfo Villafiorita. Integrating Fault Tree Analysis with Event Ordering Information. In *Proceedings of ESREL 2003*, pages 247–254, 2003.

[40] Marco Bozzano and Adolfo Villafiorita. The FSAP/NuSMV-SA Safety Analysis Platform. *Software Tools for Technology Transfer*, 9(1):5–24, 2007.

[41] Marco Bozzano and Adolfo Villafiorita. *Design and Safety Assessment of Critical Systems*. CRC Press (Taylor and Francis), an Auerbach Book, 2010.

[42] Marco Bozzano, Adolfo Villafiorita, Ove Åkerlund, Pierre Bieber, Christian Bougnol, Eckard Böde, Matthias Bretschneider, Antonella Cavallo, et al. ESACS: an integrated methodology for design and safety analysis of complex systems. *Proc. ESREL 2003*, pages 237–245, 2003.

[43] Aaron R. Bradley. SAT-Based Model Checking without Unrolling. In *VMCAI*, pages 70–87, 2011.

[44] Aaron R. Bradley and Zohar Manna. Checking safety by inductive generalization of counterexamples to induction. In *Formal Methods*

in Computer Aided Design, 2007. FMCAD'07, pages 173–180. IEEE, 2007.

[45] Robert Brayton and Alan Mishchenko. ABC: An academic industrial-strength verification tool. In *Computer Aided Verification*, pages 24–40. Springer, 2010.

[46] Manfred Broy. Towards a Theory of Architectural Contracts: - Schemes and Patterns of Assumption/Promise Based System Specification. In *Software and Systems Safety - Specification and Verification*, pages 33–87. IOS Press, 2011.

[47] Randal E. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Trans. Computers*, 35(8):677–691, 1986.

[48] Jerry R. Burch, Edmund M. Clarke, Kenneth L. McMillan, David L. Dill, and Lain-Jinn Hwang. Symbolic model checking: 10 20 states and beyond. In *Logic in Computer Science, 1990. LICS'90, Proceedings., Fifth Annual IEEE Symposium on e*, pages 428–439. IEEE, 1990.

[49] Kai-Yuan Cai. System failure engineering and fuzzy methodology an introductory overview. *Fuzzy sets and systems*, 83(2):113–133, 1996.

[50] Roberto Cavada, Alessandro Cimatti, Michele Dorigatti, Alberto Griggio, Alessandro Mariotti, Andrea Micheli, Sergio Mover, Marco Roveri, and Stefano Tonetta. The nuXmv Symbolic Model Checker. In *Proc. CAV*, pages 334–342, 2014.

[51] Alessandro Cimatti, Edmund Clarke, Enrico Giunchiglia, Fausto Giunchiglia, Marco Pistore, Marco Roveri, Roberto Sebastiani, and Armando Tacchella. NuSMV 2: An OpenSource Tool for Symbolic

Model Checking. In *Computer Aided Verification*, pages 359–364. Springer, 2002.

[52] Alessandro Cimatti, Edmund Clarke, Fausto Giunchiglia, and Marco Roveri. NuSMV: a new symbolic model checker. *STTT International Journal on Software Tools for Technology Transfer. Editors-in-Chief: B. Steffen - W. R. Cleaveland. Springer Verlag.*, pages 410–425, 2000.

[53] Alessandro Cimatti, Edmund Clarke, Fausto Giunchiglia, and Marco Roveri. NuSMV: a new Symbolic Model Checker. *International Journal on Software Tools for Technology Transfer (STTT)*, 2(4):410–425, March 2000.

[54] Alessandro Cimatti, Michele Dorigatti, and Stefano Tonetta. OCRA: A Tool for Checking the Refinement of Temporal Contracts. In *ASE*, pages 702–705. IEEE, 2013.

[55] Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. Parameter synthesis with IC3. In *Proceedings of FMCAD*, pages 165–168. IEEE, 2013.

[56] Alessandro Cimatti, Alberto Griggio, Bastiaan Joost Schaafsma, and Roberto Sebastiani. The MathSAT5 SMT Solver. In *TACAS*, pages 93–107, 2013.

[57] Alessandro Cimatti, Marco Roveri, and Stefano Tonetta. Requirements validation for hybrid systems. In *Computer Aided Verification*, pages 188–203. Springer, 2009.

[58] Alessandro Cimatti and Stefano Tonetta. A property-based proof system for contract-based design. In *Software Engineering and Advanced Applications (SEAA), 2012 38th EUROMICRO Conference on*, pages 21–28. IEEE, 2012.

[59] Alessandro Cimatti and Stefano Tonetta. Contracts-refinement proof system for component-based embedded systems. *Science of Computer Programming*, 97:333–348, 2015.

[60] Koen Claessen and Niklas Sörensson. A liveness checking algorithm that counts. In *FMCAD*, pages 52–59, 2012.

[61] Andreas Classen, Patrick Heymans, Pierre-Yves Schobbens, and Axel Legay. Symbolic model checking of software product lines. In *Proceedings of the 33rd International Conference on Software Engineering*, pages 321–330. ACM, 2011.

[62] Olivier Coudert and Jean Christophe Madre. A new method to compute prime and essential prime implicants of boolean functions. *Advanced Research in VLSI and Parallel Systems, Knight and Savage (Eds)*, pages 113–128, 1992.

[63] Olivier Coudert and Jean Christophe Madre. Fault Tree Analysis: 10^{20} Prime Implicants and Beyond. In *Proc. RAMS*, 1993.

[64] Werner Damm, Hardi Hungar, Bernhard Josko, Thomas Peikenkamp, and Ingo Stierand. Using contract-based component specifications for virtual integration testing and architecture design. In *DATE*, pages 1023–1028, 2011.

[65] Niklas Eén and Niklas Sörensson. Temporal induction by incremental SAT solving. *Electronic Notes in Theoretical Computer Science*, 89(4), 2003.

[66] E. Allen Emerson and Chin-Laung Lei. Temporal model checking under generalized fairness constraints. In *Proceedings of the 18th Annual Hawaii International Conference on System Sciences*, pages 84–96, 1985.

[67] Christian Favre. Fly-by-wire for commercial aircraft: the airbus experience. *International Journal of Control*, 59(1):139–157, 1994.

[68] Peter Fenelon, John A. McDermid, Mark Nicolson, and David J. Pumfrey. Towards integrated safety analysis and design. *ACM SIGAPP Applied Computing Review*, 2(1):21–32, 1994.

[69] Marco Gario, Alessandro Cimatti, Cristian Mattarei, Stefano Tonetta, and Kristin Y. Rozier. Model checking at scale: Automated air traffic control design space exploration. In *Under Submission*.

[70] Marco Gario and Andrea Micheli. PySMT: a solver-agnostic library for fast prototyping of SMT-based algorithms. In *SMT-Workshop*, 2015.

[71] Nouredine Hadjsaid, Marie-Cecile Alvarez-Herault, Raphael Caire, Bertrand Raison, Justine Descloux, and Wojciech Bienia. Novel architectures and operation modes of distribution network to increase dg integration. In *IEEE conference, General Meeting 2010, Minneapolis, USA*. IEEE, 2010.

[72] Masashi Hamamatsu, Tatsuhiro Tsuchiya, and Tohru Kikuno. On the reliability of cascaded TMR systems. In *Dependable Computing (PRDC), 2010 IEEE 16th Pacific Rim International Symposium on*, pages 184–190. IEEE, 2010.

[73] Gerard J. Holzmann. The model checker SPIN. *Software Engineering, IEEE Transactions on*, 23(5):279–295, 1997.

[74] Husni R. Idris, Ni Shen, and David J. Wing. Improving separation assurance stability through trajectory flexibility preservation. In *10th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference*, page 9011, 2010.

[75] Frantz Iwu, Andy Galloway, John A. McDermid, and Ian Toyn. Integrating safety and formal analyses using UML and PFS. *Reliability Engineering & System Safety*, 92(2):156–170, 2007.

[76] Jean-Baptiste Jeannin, Khalil Ghorbal, Yanni Kouskoulas, Ryan Gardner, Aurora Schmidt, Erik Zawadzki, and André Platzer. A formally verified hybrid system for the next-generation airborne collision avoidance system. In *Tools and Algorithms for the Construction and Analysis of Systems*, pages 21–36. Springer, 2015.

[77] Jonathan M. Johnson and Michael J. Wirthlin. Voter insertion algorithms for FPGA designs using triple modular redundancy. In *Proc. of the 18th annual ACM/SIGDA international symposium on Field programmable gate arrays*, pages 249–258. ACM, 2010.

[78] Kamiar Karimi. Future aircraft power systems- integration challenges. In *CMU Conference on the Electricity Industry, Feb. 2008, Pittsburg, PA.* CMU, 2008.

[79] David A. Karr, Robert A. Vivona, David A. Roscoe, Stephen M. DePascale, and David J. Wing. Autonomous operations planner: A flexible platform for research in flight-deck support for airborne self-separation. In *12th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference and 14th AIAA/ISSMO Multidisciplinary Analysis and Optimization Conference*, page 5417, 2012.

[80] Farid Katiraei. Novel microgrids management: Controls and operation aspects of microgrids. *IEEE Power Energy Magazine*, (May/June), 2008.

[81] Andrew J. Kornecki and Kimberley Hall. Approaches to assure safety in fly-by-wire systems: Airbus vs. boeing. In *IASTED Conf. on Software Engineering and Applications*, pages 471–476, 2004.

[82] Tan Lanfang, Tan Qingping, and Li Jianli. Specification and verification of the triple-modular redundancy fault tolerant system using csp. In *DEPEND 2011, The Fourth International Conference on Dependability*, pages 14–17, 2011.

[83] Donald C. Latham. Department of defense trusted computer system evaluation criteria. *Department of Defense*, 1986.

[84] Todd Lauderdale, Timothy Lewis, Thomas Prevot, Mark Ballin, Arwa Aweiss, and Nelson Guerreiro. Function allocation for separation assurance: Research plan. NASA HQ Project Overview, Aug. 2014.

[85] Christoph Lauer, Reinhard German, and Jens Pollmer. Fault tree synthesis from uml models for reliability analysis at early design stages. *ACM SIGSOFT Software Engineering Notes*, 36(1):1–8, 2011.

[86] LayerZero Power Systems, Inc. – Triple Modular Redundancy. `http://www.layerzero.com/Innovations/Industry-Firsts/Triple-Modular-Redundancy.html`.

[87] Sungjae Lee, Jae il Jung, and Inhwan Lee. Voting structures for cascaded triple modular redundant modules. *Ieice Electronic Express*, 4(21):657–664, 2007.

[88] Panagiotis Manolios, Daron Vroon, and Gayatri Subramanian. Automating component-based system assembly. In *Proceedings of the 2007 international symposium on Software testing and analysis*, pages 61–72. ACM, 2007.

[89] Evelyn Mathison and Kamiar Karimi. Power quality specification development for more electric airplane architectures. In *Power System*

Conference Proceedings, October 2002, number SAE 2002-01-3266. SAE, October 2002.

[90] Cristian Mattarei, Alessandro Cimatti, Marco Gario, Stefano Tonetta, and Kristin Y. Rozier. Comparing different functional allocations in automated air traffic control design. In *Formal Methods in Computer-Aided Design, FMCAD 2015, Austin, Texas, USA, September 27-30, 2015*, pages 112–119, 2015.

[91] Mark L. McKelvin Jr, Gabriel Eirea, Claudio Pinello, Sri Kanajan, and Alberto Sangiovanni-Vincentelli. A formal approach to fault tree synthesis for the analysis of distributed fault tolerant systems. In *EMSOFT*, pages 237–246. ACM, 2005.

[92] Kenneth L. McMillan. *Symbolic model checking*. Springer, 1993.

[93] Kenneth L. McMillan. Interpolation and sat-based model checking. In *CAV*, pages 1–13, 2003.

[94] The MISSA Project. `http://www.missa-fp7.eu`.

[95] UK MoD. The procurement of safety critical software in defence equipment. *Interim Defence Standard 00-55, UK Ministry of Defence, Directorate of Standardization, Kentigern House*, 65, 1991.

[96] Ian Moir and Allan Seabridge. *Aircraft Systems: Mechanical, Electrical and Avionics Subsystems Integration*. John Wiley & Sons, 2008.

[97] nuXmv: a new eXtended model verifier. `https://nuxmv.fbk.eu`.

[98] OpenFTA: OpenFTA is an advanced tool for fault tree analysis. `http://www.openfta.com/`.

[99] Ganesh J. Pai and Joanne Bechta Dugan. Automatic synthesis of dynamic fault trees from UML system models. In *Software Reliability Engineering, 2002. ISSRE 2003. Proceedings. 13th International Symposium on*, pages 243–254. IEEE, 2002.

[100] Yiannis Papadopoulos and John A. McDermid. Hierarchically performed hazard origin and propagation studies. In *in Lecture Notes in Computer Science, 1698:139-152, Proceedings of SAFECOMP'99, the 18 th International Conference on Computer Safety, Reliability and Security*, pages 139–152. Springer Verlag, 1999.

[101] Claudio Pinello, Luca Carloni, and Alberto Sangiovanni-Vincentelli. Fault-tolerant deployment of embedded software for cost-sensitive real-time feedback-control applications. In *DATE*, page 21164. IEEE Computer Society, 2004.

[102] Amir Pnueli. The temporal logic of programs. In *FOCS*, pages 46–57, 1977.

[103] Mukul R. Prasad, Armin Biere, and Aarti Gupta. A survey of recent advances in sat-based formal verification. *International Journal on Software Tools for Technology Transfer*, 7(2):156–173, 2005.

[104] Antoine Rauzy. New algorithms for fault trees analysis. *Reliability Engineering & System Safety*, 40(3):203–211, 1993.

[105] Antoine Rauzy. Mathematical Foundations of Minimal Cutsets. *IEEE Transactions on Reliability*, 50(4):389–396, 2001.

[106] Anish Sachdeva, Dinesh Kumar, and Pradeep Kumar. Reliability modeling of an industrial system with petri nets. In *Proceedings of ESREL*, pages 1087–94, 2007.

[107] SAE. ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, dec 1996.

[108] SAE. ARP4754A Guidelines Guidelines for Development of Civil Aircraft and Systems, dec 2010.

[109] SAE. AIR 6110, Contiguous Aircraft/ System Development Process Example, December 2011.

[110] Manel Sghairi, Agnan De Bonneval, Yves Crouzet, Jean-Jacques Aubert, and Patrice Brot. Challenges in building fault-tolerant flight control system for a civil aircraft. *IAENG International Journal of Computer Science*, 35(4), 2008.

[111] Mary Sheeran, Satnam Singh, and Gunnar Stålmarck. Checking safety properties using induction and a sat-solver. In *FMCAD*, pages 108–125, 2000.

[112] Sajjad Siddiqi and Jinbo Huang. Hierarchical Diagnosis of Multiple Faults. In *IJCAI*, pages 581–586, 2007.

[113] Ivan Sikora, Stanislav Pavlin, and Ernest Bazijanac. Flight operations and engineering documentation managing and distribution supported by intelligent transport systems. 2000.

[114] Cary R. Spitzer. *The Avionics Handbook*. CRC Press, 2000.

[115] Darshan D. Thaker, Rajeevan Amirtharajah, Francois Impens, Isaac L. Chuang, and Frederic T. Chong. Recursive TMR: Scaling fault tolerance in the nanoscale era. *Design & Test of Computers, IEEE*, 22(4):298–305, 2005.

[116] Moshe Y. Vardi and Pierre Wolper. An automata-theoretic approach to automatic program verification. In *1st Symposium in Logic in Computer Science (LICS)*. IEEE Computer Society, 1986.

[117] William E. Vesely, Joanne Bechta Dugan, Joseph Fragola, Joseph Minarick, and Jan Railsback. Fault tree handbook with aerospace applications. *NASA Office of Safety and Mission Assurance*, 2002.

[118] William E. Vesely, Francine F. Goldberg, Norman H. Roberts, and David F. Haasl. Fault tree handbook. Technical Report NUREG-0492, Systems and Reliability Research Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission, 1981.

[119] Christian von Essen and Dimitra Giannakopoulou. Analyzing the next generation airborne collision avoidance system. In *Tools and Algorithms for the Construction and Analysis of Systems*, pages 620–635. Springer, 2014.

[120] David J. Wing, Mark G. Ballin, and Karthik Krishnamurthy. Pilot in command: a feasibility assessment of autonomous flight management operations. In *24th International Congress of the Aeronautical Sciences*, 2004.

[121] Xilinx. TMRTool.

[122] Ying C. Yeh. Triple-Triple Redundant 777 Primary Flight Computer. In *Aerospace Applications Conference, 1996. Proc., IEEE*, volume 1, pages 293–307. IEEE, 1996.

[123] Miaomiao Zhang, Zhiming Liu, Charles Morisset, and Anders Ravn. Design and verification of fault-tolerant components. *Methods, Models and Tools for Fault Tolerance*, pages 57–84, 2009.

[124] Yang Zhao and Kristin Yvonne Rozier. Formal specification and verification of a coordination protocol for an automated air traffic control system. *Science of Computer Programming Journal*, 96(3):337–353, December 2014.

[125] Yang Zhao and Kristin Yvonne Rozier. Probabilistic model checking for comparative analysis of automated air traffic control systems. In *Proceedings of the 33rd IEEE/ACM International Conference On Computer-Aided Design (ICCAD 2014)*, page To appear, San Jose, California, U.S.A., November 2014. IEEE/ACM.

[126] Enrico Zio. Reliability engineering: Old problems and new challenges. *Reliability Engineering & System Safety*, 94(2):125–141, 2009.

[127] Enrico Zio and Marzio Marseguerra. Basics of the monte carlo method with application to system reliability. *LiLoLe, Hagen*, 2002.